इंटरनेट मानक

Disclosure to Promote the Right To Information

Whereas the Parliament of India has set out to provide a practical regime of right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability in the working of every public authority, and whereas the attached publication of the Bureau of Indian Standards is of particular interest to the public, particularly disadvantaged communities and those engaged in the pursuit of education and knowledge, the attached public safety standard is made available to promote the timely dissemination of this information in an accurate manner to the public.

"जानने का अधिकार, जीने का अधिकार"
Mazdoor Kisan Shakti Sangathan
"The Right to Information, The Right to Live"

"पुराने को छोड नये के तरफ"
Jawaharlal Nehru
"Step Out From the Old to the New"

IS 13968-1-1 to 5 (1994): Performance and Testing of Teleprotection Equipment of Power Systems, Part 1: Narrow Band Command Systems [LITD 10: Power System Control and Associated Communications]

"ज्ञान से एक नये भारत का निर्माण"
Satyanarayan Gangaram Pitroda
"Invent a New India Using Knowledge"

Act Number 22 of 2005
The Indian Parliament
RIGHT TO INFORMATION

Made Available By
Public.Resource.Org

"ज्ञान एक ऐसा खजाना है जो कभी चुराया नहीं जा सकता है"
Bhartṛhari—Nītiśatakam
"Knowledge is such a treasure which cannot be stolen"

BLANK PAGE

BRUTUM FULMEN

IGNORANTIA
JURIS
NON EXCUSAT

PROTECTED BY COPYRIGHT

IS 13968 (Part 1/Sec 1 to 5) : 1994

भारतीय मानक

पावर तंत्र के दूरसचार उपस्कर की कार्यकारिता और वरीयता

भाग 1 नेरो बेंड कमांड तंत्र

Indian Standard

PERFORMANCE AND TESTING OF TELEPROTECTION EQUIPMENT OF POWER SYSTEMS

PART 1 NARROW BAND COMMAND SYSTEMS

UDC 621·39·052·63 : 621·372·512

© BIS 1994

BUREAU OF INDIAN STANDARDS
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

May 1994

Price Group 11

Power Line Carrier Systems and Associated Telecontrol Equipment Sectional Committee, LTD 25

FOREWORD

This Indian Standard (Part 1/Sec 1 to 5) was adopted by the Bureau of Indian Standards, after the draft finalized by the Power Line Carrier Systems and Associated Telecontrol Equipment Sectional Committee had been approved by the Electronics and Telecommunication Division Council.

The object of this standard is to establish performance requirements and recommended methods for testing channels used for transmitting signals related to the command information required by the protective devices in power systems and to give the associated terminology.

Both the power supply belonging to the equipment and the performance of the teleprotection equipment shall be tested. All the tests should be considered as type tests.

This standard (Part 1) covers the requirements of narrow-band command systems in five sections given below:

- Section 1 General
- Section 2 Terminology
- Section 3 Definitions of Teleprotection Systems
- Section 4 Requirements
- Section 5 Methods for Performance Testing

This standard is based on IEC Pub 834-1 (1988) 'Performance and testing of teleprotection equipment of power systems : Part 1 Narrow-band command systems', issued by the International Electrotechnical Commission (IEC).

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated, expressing the result of a test or analysis, shall be rounded off in accordance with IS 2 : 1960 'Rules for rounding off numerical values (*revised*)'. The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.

Indian Standard

PERFORMANCE AND TESTING OF TELEPROTECTION EQUIPMENT OF POWER SYSTEMS

PART 1 NARROW BAND COMMAND SYSTEMS

Section 1 General

1 SCOPE

1.1 This standard (Part 1/Sec 1) covers general aspects of narrow-band single-signal and multi-signal equipment for teleprotection.

It also applies to voice frequency equipment which is used in connection with various telecommunication systems, such as power line carrier (PLC), radio link, rented circuits, leased or owned cables.

Narrow band systems include audio frequency systems operating within a 4 kHz maximum band, and PLC channels within a maximum of 4 kHz bandwidth (for one direction of transmission).

2 SERVICE CONDITIONS

2.1 Ambient Temperature and Humidity

The stated performance requirements shall be satisfied when the ambient temperature lies between 0°C and + 50°C and the relative humidity not exceeding 95 percent indoor, non-condensing.

NOTE — Special cases of relative humidity higher than 95 percent shall be covered by mutual agreement between the manufacturer and the purchaser.

2.2 Supply Voltage with Battery Operation

The stated performance requirements shall be satisfied when the supply voltage lies between − 10 percent and + 15 percent of its nominal value.

The terminal shall remain operational when the supply voltage rises by 20 percent of its nominal value.

NOTE — The variation figures coated are typical for lead-acid batteries, the nominal voltage being taken as 2·0 V per cell.

2.3 Supply Voltage with ac Mains Operation

The stated performance requirements shall be satisfied when the supply voltage lies between ± 15 percent of its nominal value. The frequency may lie between 45 Hz and 53 Hz with a maximum distortion factor of 5 percent.

3 TELECOMMUNICATION CIRCUIT USED

3.1 Figure 1 shows the configuration of teleprotection equipment working at an audio frequency band (using part of a 4 kHz baseand). The signals are conveyed from the transmitter to the receiver via a telecommunication circuit.

The telecommunication circuit can be:

a) cable link for audio frequency transmission;

b) carrier frequency links for cables and overhead lines;

c) carrier frequency links on aerial cables on power lines;

d) power line carrier links (PLC);

e) point-to-point radio links (microwave);

f) rented circuits; and

g) optical waveguides (fibre optics).

The telecommunication circuits should be chosen with care, as they will be influenced by noise, change of parameters and any kind of interference which may cause maloperation or nonoperation of the teleprotection equipment.

Figure 2 shows the configuration when the guard and command signals are generated and received at Power Line Carrier Frequencies.

Figures 1 and 2 apply to both frequency shift and normally quiescent systems.

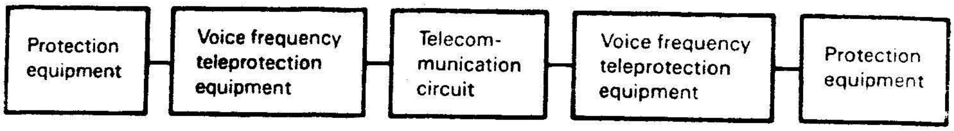

Protection equipment
Voice frequency teleprotection equipment
Telecom-munication circuit
Voice frequency teleprotection equipment
Protection equipment

FIG. 1 AUDIO FREQUENCY CONFIGURATION

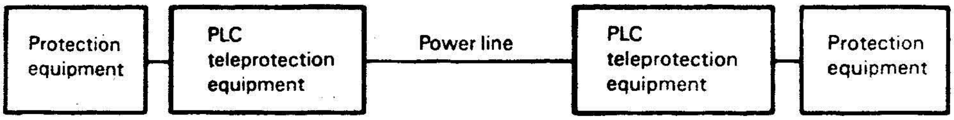


FIG. 2 CARRIER FREQUENCY CONFIGURATION

Indian Standard

PERFORMANCE AND TESTING OF TELEPROTECTION EQUIPMENT OF POWER SYSTEMS

PART 1 NARROW BAND COMMAND SYSTEMS

Section 2 Terminology

1 SCOPE

1.1 This standard (Part 1/Sec 2) covers definitions of fundamental terms relating to narrow band command systems for teleprotection.

1.2 Figure 1 is intended to clarify the concepts and the relations among terms in use.

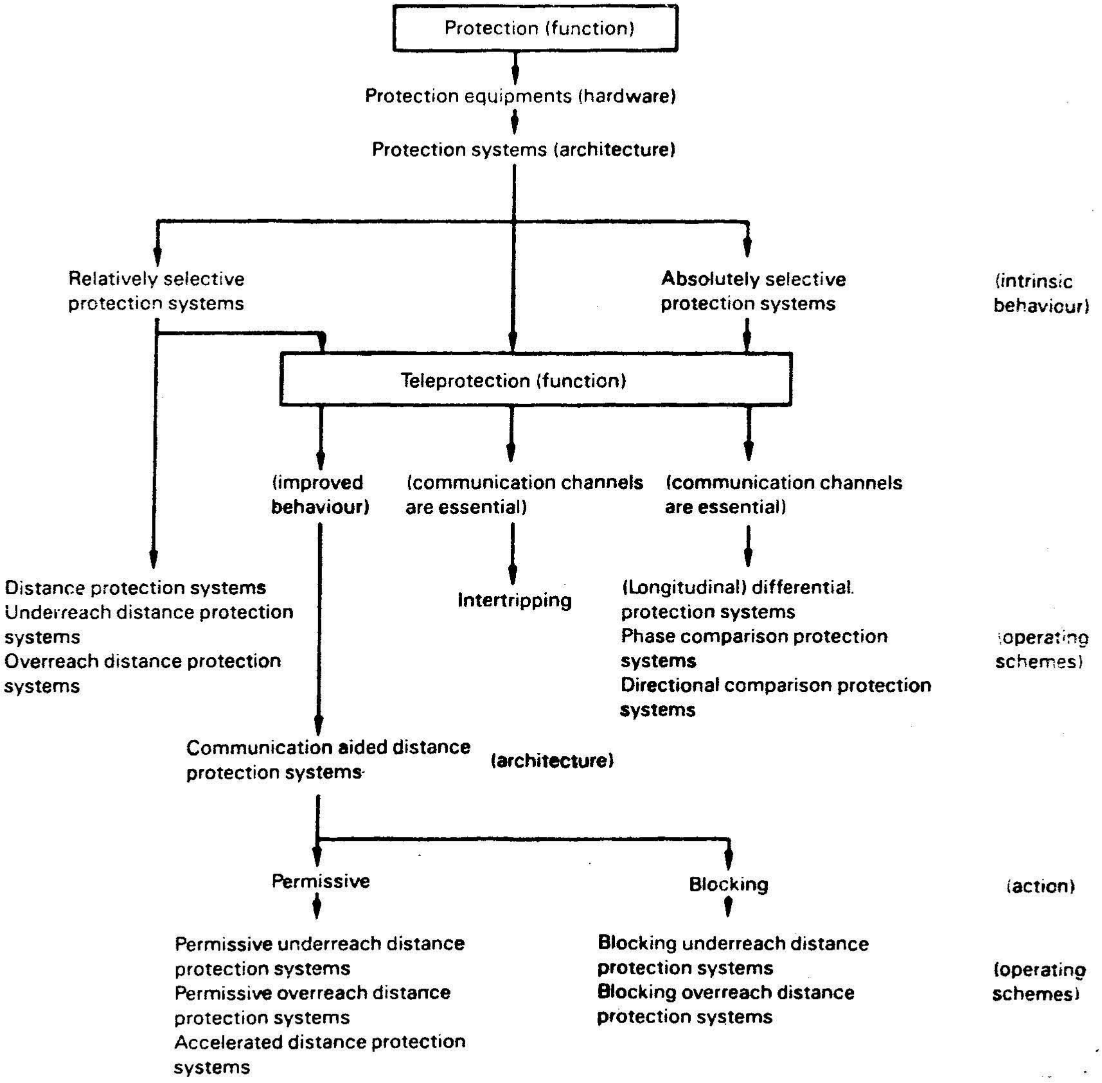

Protection (function)
Protection equipments (hardware)
Protection systems (architecture)
Relatively selective protection systems
Absolutely selective protection systems
(intrinsic behaviour)
Teleprotection (function)
(improved behaviour)
(communication channels are essential)
(communication channels are essential)
Distance protection systems
Underreach distance protection systems
Overreach distance protection systems
Intertripping
(Longitudinal) differential protection systems
Phase comparison protection systems
Directional comparison protection systems
(operating schemes)
Communication aided distance protection systems
(architecture)
Permissive
Blocking
(action)
Permissive underreach distance protection systems
Permissive overreach distance protection systems
Accelerated distance protection systems
Blocking underreach distance protection systems
Blocking overreach distance protection systems
(operating schemes)

FIG. 1 FUNDAMENTAL TERMS ON PROTECTION AND TELEPROTECTION

2 GENERAL TERMS

2.1 Protection

Protection normally expected to take the initiative in case of a fault in the protected zone.

2.2 Protection Equipment

Hardware of protection.

2.3 Protection System

Architecture for protection.

2.4 Selectivity (for a Protection System)

Protection which determines that the fault is within its own zone and isolates that zone only.

NOTE — Selectivity means the ability to determine whether or not operation is required and enables to obtain optimum isolation consistent with the conditions of fault. The selectivity is absolute if the protection responds only to faults within its own zone, and relative if it is obtained by grading the settings (for example, time or current) of the protection of several zones all of which may respond to a given fault.

2.5 Distance Protection System

The protection operation of which depends upon the impedance of the circuit between the relaying point and the point of fault; the terms being generalized from its wide application to transmission lines.

2.5.1 *Definite Distance Protection*

Distance protection which operates up to a specified value of impedance and does not operate at higher values.

2.5.2 *Stepped Curve Distance*

Time Protection—Distance Protection of which the time-lag is a stepped function of the distance measured, the latter being correspondingly subdivided into several steps or zones.

2.5.3 *Basic Time*

The shortest operating time of distance protection, for example, the time of the first step or zone in a stepped curve distance-time protection.

2.5.4 *Time Limit* (*for Distance Protection*)

The operating time corresponding to the last step or zone.

2.5.5 *Reach* (*for Stepped Curve Distance—Time Protection*)

The distance corresponding to the farther end of each step or zone.

3 TELEPROTECTION

3.1 Teleprotection Equipment

Equipment specially designed to be used in conjunction with a protection system requiring a telecommunication link between the ends of the protected circuit, to transform the information given by the protection equipment in a way suitable for transmission.

a) *Teleprotection System*

System composed by the teleprotection equipment and associated telecommunication system needed, in a protection system requiring a telecommunication link between the ends of the protected circuit.

b) *Teleprotection Channel*

1) The frequency band at disposal on the telecommunication system in order to permit the transmission of protection signals in both directions.
2) System composed, for testing purposes by teleprotection equipment connected back-to-back without the associated telecommunication system.

c) *Telecommunication System — Telecommunication Link*

System composed by telecommunication equipment and the associated physical link needed to transmit information signals over the distance.

3.2 Pilot Wire Protection System

Protection based upon a comparison of the corresponding electrical quantities at each terminal of the protected zone, through the agency of communicating means; such as pilot-wire, carrier-current and a radio-link.

3.2.1 *Pilot Protection System*

Pilot protection in which an auxiliary metallic circuit is used as the communicating means between the terminals of the protected zone.

3.2.2 *Pilot Protection with Direct Comparison*

Pilot protection in which the pilot-wire link transmits directly the characteristic quantities.

3.2.3 *Pilot Protection with Indirect Comparison*

Pilot protection in which the pilot-wire link transmits from one end to the other a signal to lock or release elements of the protection.

3.2.4 *Phase-Comparison Protection*

Pilot protection in which quantities compared are the phase angles of the currents or voltages at the terminals of the protected zone.

3.2.5 *Carrier-Current Protection*

Pilot protection in which high-frequency current transmitted over the protected zone provides the means of communication between its terminals.

3.2.6 *Radio-Link Protection*

Pilot protection in which radio-borne signals are used for communication between the terminals of the protected zone.

3.3 Blocking Protection System

An element of protection which under certain conditions prevents or limits the operation of other elements.

3.4 (Longitudinal) Differential Protection System

Differential protection in which the differential current equals the algebraic sum of the currents flowing into the protected zone.

3.5 Directional Comparison Protection System

Power protection which operates in accordance with the direction of the power but is substantially independent of its magnitude.

3.6 Intertripping

A method in which the tripping of the circuit-breaker at one end of a circuit is initiated by a signal transmitted from the protection at the other end.

Indian Standard

PERFORMANCE AND TESTING OF TELEPROTECTION EQUIPMENT OF POWER SYSTEMS

PART 1 NARROW BAND COMMAND SYSTEMS

Section 3 Definitions of Teleprotection Systems

1 SCOPE

1.1 This standard (Part 1/Sec 3) deals with the terms used in the description and/or specification of teleprotection systems.

2 TYPES OF TELEPROTECTION SCHEMES

2.1 Permissive Trip Schemes

This term denotes channels operating in an audio frequency band, or in a PLC frequency band. The channel is designed with the premise that the dependability of operation is high even under conditions when, due to a power system disturbance, the telecommunication medium may be adversely affected. Frequency shift signalling with or without coding techniques is usually employed.

2.2 Intertripping Schemes (Direct Trip)

Intertrip channels are similar in operation to permissive trip channels with the exception that security against unwanted operation and dependability of correct operation are prime requirements. Speed of operation is usually sacrificed to meet security and dependability requirements.

2.3 Blocking Protection Schemes

These channels are similar to permissive trip channels, except in the more stringent requirement for dependability of operation and in the seed requirement.

3 OVERALL OPERATING TIME OF TELEPROTECTION SYSTEMS (TELECOMMUNICATION CIRCUIT INCLUDED)

Overall operating time T is the time elapsed between the moment of change of state at the transmitter input and the moment of the corresponding change of state at the receiver output including propagation time and additional delay due to noise.

Overall operating time is part of the fault clearance time (*see* Fig. 1).

NOTE — Fault clearance time T_c is shown in Fig. 1 as typical only.

4 TRANSMISSION TIME (TELECOMMUNICATION CIRCUIT EXCLUDED)

4.1 The transmission time of a teleprotection channel is the time elapsed between the moment of change of state at the transmitter input and the moment of the corresponding change of state at the receiver output excluding propagation time. The nominal transmission time is normally specified for a noise-free transmission path and implies zero loss probability.

The transmission time of a particular change of state can be related to a specified loss probability, which is the same as specifying the probability that a certain delay is exceeded.

The transmission time is then measured with continuous white noise applied to the transmission path; for various S/N (Signal-to-noise) ratios it is determined as the delay corresponding to a specified loss rate (typically 7 ms-65 ms).

This method corresponds to reality to a certain extent, since the probability of excessive delay is crucial to the user.

4.1.1 *Nominal Transmission Time for a Teleprotection Channel* (T_0)

This is the time elapsed from the initiating of the input of a teleprotection transmitter until the teleprotection receiver has given an output measured under noise-free conditions.

4.1.2 *Maximum Actual Transmission Time for a Teleprotection Channel* (T_{ac})

This is the maximum time elapsed from the initiating of the input of a teleprotection transmitter until the teleprotection receiver has given an output, measured under noisy conditions for a defined dependability and S/N ratio (clamping action with influence the additional delay due to noise).

5 SECURITY

Security means the ability to prevent interference and noise from generating a command state at the receiving end when no command signal is transmitted.

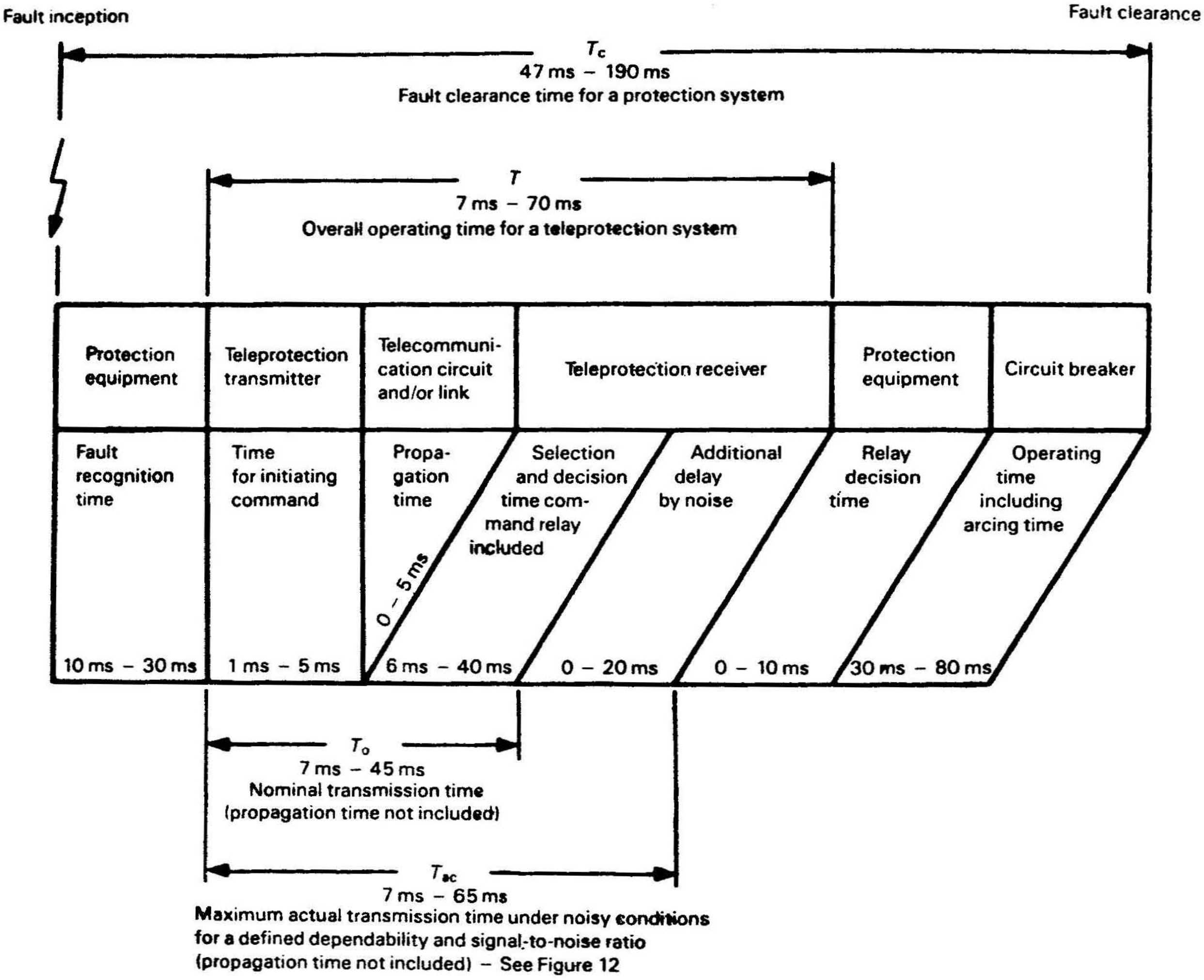

Fault inception
Fault clearance
T_c
47 ms – 190 ms
Fault clearance time for a protection system
T
7 ms – 70 ms
Overall operating time for a teleprotection system
Protection equipment
Teleprotection transmitter
Telecommunication circuit and/or link
Teleprotection receiver
Protection equipment
Circuit breaker
Fault recognition time
Time for initiating command
Propagation time
Selection and decision time command relay included
Additional delay by noise
Relay decision time
Operating time including arcing time
0 – 5 ms
10 ms – 30 ms
1 ms – 5 ms
6 ms – 40 ms
0 – 20 ms
0 – 10 ms
30 ms – 80 ms
T_o
7 ms – 45 ms
Nominal transmission time (propagation time not included)
T_{ac}
7 ms – 65 ms
Maximum actual transmission time under noisy conditions for a defined dependability and signal-to-noise ratio (propagation time not included) – See Figure 12

FIG. 1 TYPICAL OPERATING TIMES FOR PROTECTION SYSTEMS

For practical reasons the probability of unwanted command P_{uc} is normally measured.

Security is then given by:

$$1 - P_{uc}$$

An unwanted command is a command that occurs at the receiving end for a time longer than a specified duration when no such command has been transmitted.

With tripping schemes, if the duration of an unwanted command state (T_{uc}) is longer than a specified duration, it will be considered as an actual command by the protection relay. With permissive trip schemes, the risk of an unwanted tripping action is generally low, while in direct trip application each unwanted command will lead to an unwanted tripping action.

With blocking schemes, unwanted command may lead, according to its duration (T_{uc}), either to a delay to trip or to prevent a necessary tripping action from taking place.

The probability of unwanted command is measured by applying bursts of white noise to the transmission path; for various S/N ratios the unwanted command rate is then determined as the ratio of the number of received commands to the number of noise bursts of specified duration applied. This method also corresponds to some extent to reality (breaker and isolator operations, arcing noise, etc) and allows comparison of results obtained with different equipment. It is essential that the unwanted command rate is measured in this way, i.e. with bursts of noise, since the receiver under test may block its output after a certain time in the presence of continuous noise.

6 DEPENDABILITY

Dependability broadly means the ability to issue a valid command in the presence of interference and/or noise.

For practical reasons the probability of missing command P_{mc} is normally measured.

Dependability is then given by:

$$1 - P_{mc}$$

When a command occurs at the transmitting end, it is considered as a missing one in the following three cases:

a) total absence of command state at the receiving end;

b) command state at the receiving end taking place with an excessive delay; and

c) too short or interrupted command state at the receiving end.

Cases (a) and (b) will obviously give a missing command for both tripping and blocking schemes.

Concerning case (c) — For a tripping scheme, if the received command is shorter than a minimum duration, the command is considered to be missing.

For a blocking scheme, a too short or interrupted command may lead to an unwanted trip on a healthy line.

The probability of missing command is measured by applying continuous white noise to the transmission path; for various S/N ratios the missing command rate is then determined from the number of commands not received within the specified time (and of specified minimum duration) divided by the number of transmitted commands.

To a certain extent this method corresponds to reality; it offers further the advantage that results obtained with different equipment can be easily compared.

7 NOMINAL FREQUENCY BAND

The nominal frequency band is the bandwidth required by the teleprotection signalling equipment to perform its stated function, including any noise sensing requirement. It affects the transmission time and the relationship between the equipment and other services using the same signalling channel.

8 NOMINAL IMPEDANCE

The nominal impedance of teleprotection equipment is defined as the input and output impedance of the equipment measured within its nominal frequency band. This impedance is normally 600 and shall rise outside the nominal frequency band to per mm parallel operation of other signals on the same telecommunication medium. In the case of protection channel operating at carrier frequencies the nominal impedance shall be the same as that for other power line carrier equipment (*see* IS 9482 : 1980 Characteristic values of inputs and outputs of single sideband PLC terminals).

9 GUARD-COMMAND SIGNALS

The guard signal being transmitted by the teleprotection equipment and is used to monitor the integrity of the telecommunication link as to level and S/N ratio requirements, and when present inhibits any output of the teleprotection receiver. The command signal is that signal transmitted by the teleprotection equipment requiring action at the receiving end as noted in 2 of Part 1/Sec 3.

10 LEVELS OF GUARD SIGNALS

In the case of dedicated teleprotection equipment the level of a guard signal is related to the power output of the transmitter in order to comply with its peak envelope power (PEP). In the case of PLC voice frequency equipment, other services may be carried of the same link on a multi-purpose basis; when a starting relay is operating the guard signal may be boosted to the full power of the transmitter, cutting other signals for the short time of the teleprotection operating.

Boosting of the guard signal is also employed on some dedicated systems, such as quiescent systems or those employing PLC high frequency teleprotection equipment.

11 LEVELS OF COMMAND SIGNALS

In the case of dedicated teleprotection equipment the level of the command signal as for the guard signal, is related to the peak envelope power (PEP) of the transmitter.

In all cases, where power boosting is applied for guard signals the same applies for command signals.

As in the Original Standard, this Page is Intentionally Left Blank

Indian Standard

PERFORMANCE AND TESTING OF TELEPROTECTION EQUIPMENT OF POWER SYSTEMS

PART 1 NARROW BAND COMMAND SYSTEMS

Section 4 Requirements

1 SCOPE

1.1 This standard (Part 1/Sec 4) specifies performance requirements of narrow-band signal equipment for teleprotection.

2 GENERAL EQUIPMENT INTERFACE REQUIREMENTS

2.1 Insulation

All input and output circuits not connected to earth (power supply terminals included) must sustain for the duration of 1 min without any damage a sinusoidal voltage at a frequency of 50 Hz-60 Hz applied between the relative terminals in parallel and earth.

For transmit and receive terminals and power supply input terminals for voltages less than 60 V, a test voltage of 500 V rms shall be used. For d.c. supply voltages greater than or equal to 60 V and a.c. power supply input terminals, a test voltage of 2 000 V rms shall be used.

For d.c. signal terminals and alarm circuit terminals connected to the protection equipment, a test voltage as under shall be used:

- a test voltage of 1 kV for operating voltage of $\leqslant$ 60 V;
- a test voltage of 1·5 kV for operating voltage of 127 V;
- a test voltage of 2·0 kV for operating voltage of 250 V.

The insulation resistance of the above-mentioned circuits, measured at the voltage of 500 V d.c., shall be not less than 100 M for any temperature less than + 35°C and relative humidity less than 75%.

2.2 Impulse Withstand Level

All input and output circuits, power supply terminals included, must sustain without any damage or unwanted change of state from guard to command output, impulse voltages applied to the relative terminals both in differential and in common mode.

The peak value of the standard test impulse of waveform 1·2/50 shall be:

- 1 kV for transmit and receive terminals and for d.c. power supply terminals less than 60 V;
- 5 kV for d.c. power supply terminals greater than or equal to 60 V for a.c. power supply terminals and for d.c. signal terminals and alarm circuit terminals connected to the protection equipment.

The test voltage levels are measured before the circuit to be tested is connected to the circuit terminals. In the case where the circuit under test presents appreciable current flows due to impulse testing (e.g. due to low impedance or surge arresters); the energy delivered by the generator must be equal to 0·5 J ± 10%.

2.3 High-Frequency Disturbance Level

All input and output circuits, power supply terminals included, must sustain, without any damage or unwanted change of state from guard to command output, damped oscillatory waveforms applied to the relative terminals both in differential and in common mode.

The frequency of the waveform shall be 1 MHz with the envelope decaying to 50% of peak value at the end of three to six cycles. The repetition rate shall be 400 per second and the duration of the test shall be at least 2 s. Other repetition rates may be agreed upon between the user and the manufacturer.

The standard peak value of the test voltage shall be:

For transmit and receive terminals and d.c. power supply input terminals for voltages less than 60 V:

- 1·0 kV for common (longitudinal) mode;
- 0·5 kV for differential (transverse) mode;

for d c. signal terminals and alarm circuit terminals connected to the protection equipment, for d.c. power supply terminals for voltages greater than or equal to 60 V and the a.c. power supply terminals:

- 2·5 kV for common (longitudinal) mode;
- 1·0 kV for differential (transverse) mode.

The test shall be carried out under operating conditions.

3 SPECIFIC POWER SUPPLY REQUIREMENTS

3.1 Power Supply Variations

All teleprotection apparatus must sustain (without either any damage or malfunctioning such as unwanted command) slow variations of the power supply voltage from nominal value to zero and zero to nominal value.

3.2 Interruptions

All teleprotection equipment shall sustain (without any malfunctioning such as unwanted command) short interruptions in the power supply voltage not longer than 20 ms occurring in random sequence for a period not longer than 20 s. No command must occur if the power is switched off for a longer time and then switched on.

3.3 Reflected Noise

If the teleprotection equipment is supplied from a d.c. source, connected as specified in **2.3**, the noise measured across the power supply terminals of the equipment under test shall not be greater than either 3 mV psophometrically weighed or 10 mV peak-to-peak.

3.4 Reverse Polarity

If the teleprotection equipment is supplied from a d.c. source, reverse polarity protection shall be provided to take care of casual inversion of power supply voltage.

4 REQUIREMENTS FOR THE TELEPROTECTION SYSTEM PERFORMANCE

4.1 Interrelationship of Requirements

Dependability, security and transmission time of a given protection signalling equipment are interdependent parameters; for a constant bandwidth, for instance, security can only be improved at the expense of dependability or transmission time.

The requirements to be met by protection signalling equipment, and therefore the optimum compromise among parameters, depend on the particular application (blocking, permissive tripping or intertripping), a further parameter being the type of transmission path used and thus the S/N ratio which has to be handed by the protection signalling channel, both in the guard and command state.

The tendency for duplication of line protection in EHV systems (to improve the overall dependability) may again influence the compromise towards higher security of the single equipment. The performance of the teleprotection equipment shall be given in the form of curves showing:

— *for dependability*:

P_{mc}: probability of missing command as a function of the S/N ratio given in decibels for different values of T_{ac};

— *for security*:

P_{uc} : probability of unwanted command as a function of the S/N ratio given in decibels.

Examples are given Fig. 8 and 11 of Part 1, Sec 5 of this standard.

The explanations and figures as mentioned are guiding values for the user for the purpose of planning various protection schemes.

4.1.1 *Blocking*

This class of protection is based on the principle of detecting 'outward' fault current flow at one end of the protected circuit if the fault is external. This causes transmission of a blocking command which prevents a possible tripping action at the other end where the current flow is 'inward'.

Either end may block the other(s), and the protection signalling equipment need not be able to receive while transmitting.

In blocking system the information link is an essential feature for avoiding unwanted tripping on external faults. To obtain correct blocking action, the tripping at the end feeding 'inward' current must be delayed sufficiently to ensure that the blocking command from the end feeding 'outward' current can be received.

On internal faults, the fault current flow is 'inward' at both ends and blocking commands are suppressed. Failure of the information link does not generally affect the ability of the protection to trip correctly.

The general requirement for a protection signalling equipment in blocking applications is, therefore, that it should be fast and dependable, since inadequate speed or dependability may cause spurious tripping on external faults. Inadequate security may cause delayed tripping on internal faults; such delays should be kept short by proper equipment design.

Maximum actual transmission time : T_{ac} less than 20 ms

— *for dependability*:

missing command probability for

$$T_{ac} : P_m < 10^{-3}$$

— *for security*:

unwanted command probability for

$$T_B = 200 \text{ ms}$$

(T_B = length of burst of white noise):

$$P_{uc} = 10^{-1} \ldots 10^{-2}$$

Unblocking protection schemes are based on the same principles as blocking schemes, but with opposite command criteria. In normal conditions a blocking command is continuously transmitted.

The general requirements in respect of dependability and security are the same as in blocking applications, whereas the nominal transmission time may be slightly higher.

Unblocking schemes are sometimes used in addition to PLC permissive tripping schemes to improve the overall dependability under marginal conditions, such as extreme additional attenuation due to the line fault.

4.1.2 *Permissive Tripping (Under Reaching)*

This protection scheme is based on the principle of detecting 'inward' fault current flow at least at one end of the protected circuit. This initiates tripping at least at one end and causes transmission of a trip command. At the other end the received command initiates tripping action in conjunction with some local fault detecting device.

Either end may trip the other(s), and the protection signalling equipment need not be able to receive while transmitting.

In permissive underreaching schemes, the information link is a supplementary feature for obtaining fast tripping at both ends for all internal fault positions. Failure of the information link does not affect the selectivity, but delays tripping at one end for certain fault locations.

On external faults no trip commands are transmitted, and failure of the information link generally does not affect the ability of the protection to stabilize correctly. However, interference and noise may cause unwanted tripping.

4.1.3 *Permissive Tripping (Overreaching)*

This class of protection is based on the principle of detecting 'inward' fault current flow at both ends of the protected circuit. This causes transmission of a trip command from each end; at the other end the received command initiates tripping action in conjunction with the local fault detecting device.

Each end must trip the other(s), and the protection signalling equipment must be able to receive while transmitting.

In permissive overreaching schemes, the information link is an essential feature for obtaining fast tripping at both ends on all internal faults. Failure of the information link may affect the selectivity and delay tripping at least at one end for all fault positions.

On external faults, the end feeding 'outward' current transmits no trip command. This prevents a possible tripping action at the other end feeding 'inward' current, and failure of the information link does not generally affect the ability of the protection to stabilize correctly. However, interference and noise may cause unwanted tripping.

The general requirement for a protection signalling equipment in permissive tripping applications is that it should be secure and fast; in overreaching schemes there is a further stress on dependability. Inadequate security may cause unwanted tripping on external faults; inadequate speed or dependability may cause delayed tripping on all internal faults or even unselectivity in overreaching schemes.

4.1.3.1 *Maximum actual transmission time*

T_{ac} less than 40 ms

— ***for dependability* (*underreaching*):**

missing command probability for

$$T_{ac} : P_{mc} < 10^{-2}$$

— ***for dependability* (*overreaching*):**

missing command probability for

$$T_{ac} \cdot P_{mc} < 10^{-2} \ldots 10^{-3}$$

— ***for security* (*underreaching*):**

unwanted command probability for

$$T_B = 200 \text{ ms} : P_{uc} < 10^{-3} \ldots 10^{-4}$$

— ***for security* (*over reaching*):**

unwanted command probability for

$$T_B = 200 \text{ ms} : P_{uc} < 10^{-3}$$

4.1.3.2 *Intertripping (transfer tripping)*

Various conditions on a power system may require a circuit breaker to be tripped remotely from a protection-relay. This applies for instance where transformers or reactors are connected to the system without circuit breakers, for breaker back-up protection and in direct tripping underreaching schemes.

The received command has complete ability to trip without any additional control and, therefore, the security of the protection signalling equipment is most important to avoid unwanted tripping. Since command transmission may be required during fault conditions, dependability is also very important for obtaining wanted tripping in the presence of noise and interference.

The general requirement for a protection signalling equipment in intertripping applications is, therefore, that it should be very secure and very dependable, since both inadequate security and dependability may cause unwanted operation. In some applications the equipment must be able to receive while transmitting, and commands may be transmitted for a longer period of time.

Maximum actual transmission time:

T_{ac} less than 60 ms

— *for dependability*:

missing command probability for

$T_{ac} : P_{mc} < 10^{-3} \ldots 10^{-4}$

— *for security*:

unwanted command probability for

$T_B = 200 \text{ ms} : P_{uc} = 10^{-5} \ldots 10^{-6}$

4.2 Monitoring and Alarms

The design of teleprotection systems and the way in which information links are used need to take account of practical limitations arising from the fact that the influence of interference, noise and communication failures cannot be completely avoided.

In many cases it is desirable to put more emphasis on dependability than on security. The balance between the risk of 'unwanted commands' and the risk of 'missing commands' largely depends on basic considerations, such as the requirements of the power system and the characteristics of the protection system associated with it.

While transmitting and receiving signals in any state assigned to a protection signalling equipment, these signals shall serve to monitor the transmission path and as much of the terminal equipment as possible. Failure to receive the transmitted signal, whether by failure of the transmission path or the terminal equipment, shall be detected by monitoring circuits associated with the receiver and transmitter. In addition, an alarm shall be initiated, provided that the period of failure exceeds a specified time (some seconds). The monitoring circuits may further respond to excessive interference and noise impairing correct operation. Again, an alarm shall then be initiated, should the period of interference exceed the specified time.

Facilities shall be provided for clamping the receiver output when the monitoring circuits have responded to some abnormal conditions. The receiver output shall be clamped in either the state that existed prior to the signal failure, or in a steady 'command off' or 'command on' state (selectable). The clamping action may be immediate or delayed (e.g. controlled by the alarm circuit).

The proper functions of monitoring and alarm circuits shall be checked in conjunction with the performance tests.

Indian Standard

PERFORMANCE AND TESTING OF TELEPROTECTION EQUIPMENT OF POWER SYSTEMS

PART 1 NARROW BAND COMMAND SYSTEMS

Section 5 Methods for Performance Testing

1 SCOPE

1.1 This standard (Part 1/Sec 5) applies to narrowband single-signal and multi-signal equipment for teleprotection.

2 GENERAL EQUIPMENT INTERFACE TESTS

2.1 Insulation

This test has to be done with the equipment under test ready to operate but without power supply.

The terminals of the circuit under test shall be put in parallel and tested to earth with an alternating voltage at power frequency having the relevant value and applied for the duration of 1 min.

After this a control test is done with an ohmmeter operating at 500 V d. c. in order to verify that the insulation resistance between the terminals in parallel and earth is higher than the prescribed value of 100 M Ω.

Finally, if the control test is satisfactory, the equipment is switched into service and normal operation is verified.

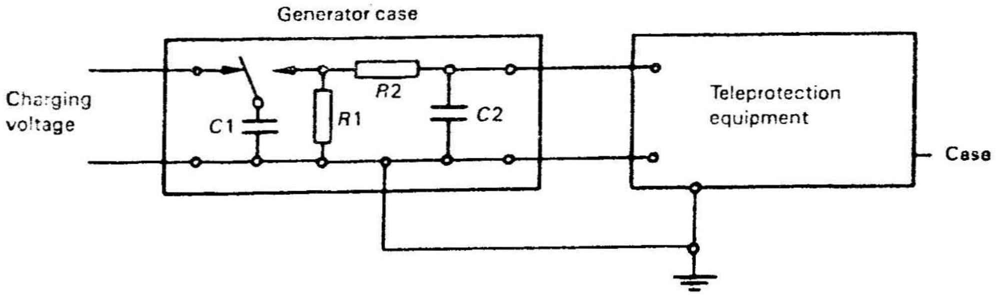
2.2 Impulse Withstand Level

Suitable impulse generators are to be adopted in order to obtain the prescribed open circuit wave shape and to give the prescribed energy in the circuit under test. The recommended test circuit is shown in Fig. 1.

Three positive impulses and three negative impulses shall be applied to the circuits.

The impulse test shall be applied:

a) between all terminals connected together and earth (common or longitudinal mode);



Components	Test Conditions		
	5 kV	2·5 kV	1 kV
*R*1	1 800 Ω	450 Ω	80 Ω
*R*2	500 Ω	500 Ω	500 Ω
*C*1	0·035 µF	0·16 µF	1·0 µF
*C*2	0·000 8 µF	0·000 8 µF	0·000 8 µF

FIG. 1 CIRCUIT FOR IMPULSE GENERATOR

b) between all independent circuits of the equipment with the terminals of each independent circuit connected together (common or longitudinal mode);

c) between terminals of the same circuit except contact circuits (differential or transverse mode).

NOTE — It is not always necessary to apply the impulse withstand test between open metallic contacts. The requirement should be agreed between the manufacturer and the user and the manufacturer should assign to the contact circuit a test voltage class.

If it is necessary to avoid the circulation of direct current in the impulse generator and an external circuit is connected to the terminals under test, the test may be executed as indicated in Fig. 2 and Fig. 3 introducing high value capacitors in order not to vary the wave shape of the impluses.

The test on the d. c. power supply terminals shall be done both with the equipment ready to operate but not switched on, and with the equipment switched on and in operation. In this latter case the circuit shall be as in Fig. 4.

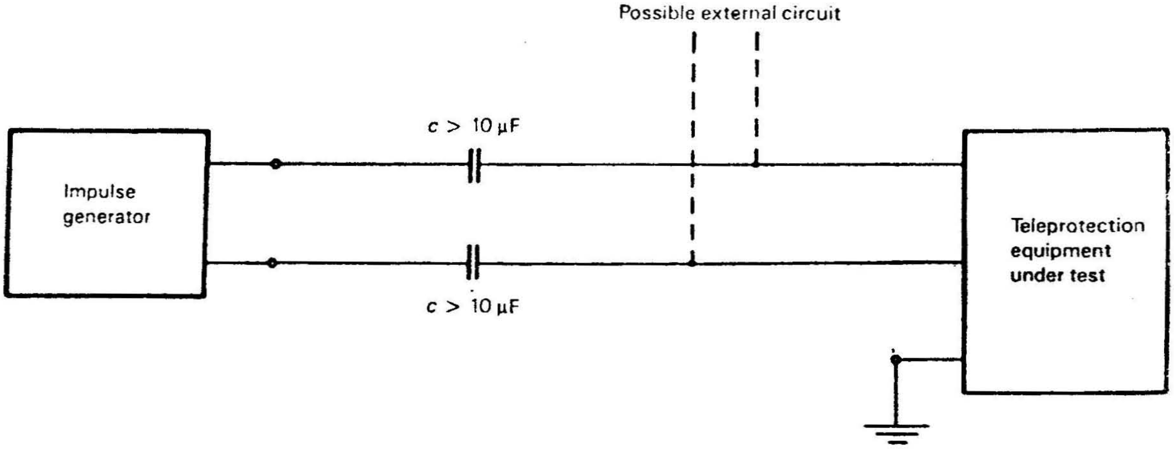

Possible external circuit
c > 10 µF
Impulse generator
c > 10 µF
Teleprotection equipment under test

FIG. 2 CIRCUIT CONFIGURATION FOR DIFFERENTIAL MODE IMPULSE WITHSTAND TEST WITH BLOCKING OF d. c. CIRCULATION ON IMPULSE GENERATOR

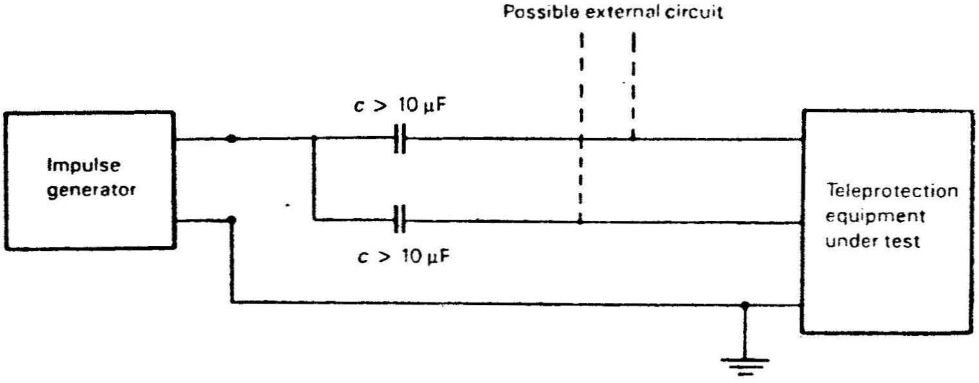

Possible external circuit
c > 10 µF
Impulse generator
c > 10 µF
Teleprotection equipment under test

FIG. 3 CIRCUIT CONFIGURATION FOR COMMON MODE IMPULSE WITHSTAND TEST WITH BLOCKING OF d. c. CIRCULATION OF IMPULSE GENERATOR

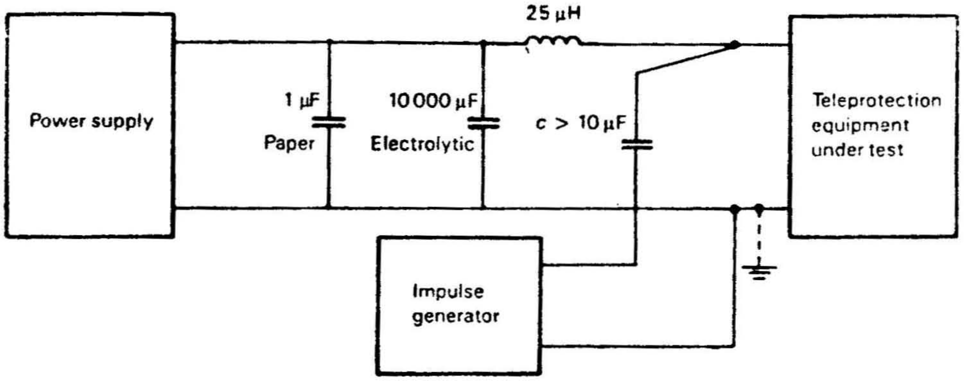


FIG. 4 CIRCUIT CONFIGURATION FOR IMPULSE WITHSTAND TEST ON d.c. POWER SUPPLY TERMINALS

After the impulse withstand tests, the equipment is put in operation and checked for correct operation and absence of unwanted operation.

2.3 High Frequency Disturbance Level

Suitable generators are to be adopted in order to obtain the prescribed upon circuit wave shape. The recommended standard test circuit is shown in Fig. 5.

The tests shall be applied:

a) between each set of input or output terminals and earth (common or longitudinal mode);

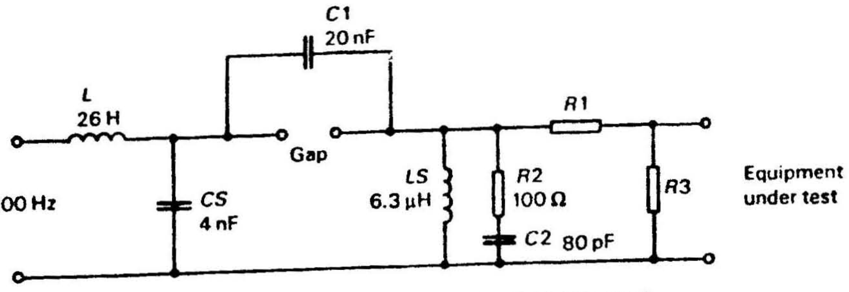
b) between all independent circuits of the equipment (common or longitudinal mode);

c) between terminals of the same circuit where applicable (differential or transverse mode);

NOTE — It is not always necessary to apply the impulse withstand test between open metallic contacts. The requirement should be agreed between the manufacturer and the user and the manufacturer should assign to the contact circuit a test voltage class.

When an external circuit is connected to the terminals under test and it is necessary to avoid the circulation of direct current in the waveform generator, the test may be executed as indicated in Fig. 2 and 3, introducing high value capacitors in order not to vary the wave shape of the test voltage.

The test on the d. c. power supply terminals shall be done both with the equipment ready to operate but not switched on, and with the



Components	Test Conditions		
	2·5 kV	1·0 kV	0·5 kV
*R*1	200 Ω	500 Ω	1 000 Ω
*R*3	∞ Ω	333·3 Ω	250 Ω

FIG. 5 CIRCUIT FOR HIGH FREQUENCY DISTURBANCE GENERATOR

equipment switched on and in operation. In this latter case the circuit shall be as in Fig. 4.

After the high frequency disturbance tests, the equipment is put in operation and checked for correct operation and absence of false operations.

3 SPECIFIC POWER SUPPLY TESTS

3.1 Power Supply Variations

In this test slow power supply voltage variations exceeding the lower limit of supply tolerances are taken into account. The variation rate shall not be faster than 10 s when the voltage changes from nominal value to zero or *vice-versa*. The aim of the test is to check that these variations do not cause unwanted commands.

It applies to both d.c. and a.c. power supplies. During the test the proper operation of the alarm device shall be checked.

It is recommended that the test be performed on the transmitter and on the receiver independently, with separate power supply units.

3.2 Interruptions

The aim of the test is to simulate the short interruptions caused for instance by loose connections in power supply wiring. They can be generated by an electronic switch, as indicated in Fig. 6.

In order in approach the random sequence of real interruptions, the pseudo-random pattern generator of a data transmission test set can be used to drive the electronic switch.

Different interruption durations, according to the selected data rate, are obtained in this way. For the 2047 bit pattern the following lengths can be achieved:

Data Rate (Bauds)	*Interruption Duration* (ms)
600	1·67 to 16·7
1 200	0·83 to 8·3

These interruptions shall not cause any unwanted command.

Disconnection of the power supply followed by reconnection after 1 min shall also not cause any unwanted command.

The interruptions test shall not cause any unwanted commands in the receiver.

3.3 Reflected Noise

An arrangement for the measurement of the noise generated by the euipment and introduced into the external power supply source is indicated in Fig. 7.

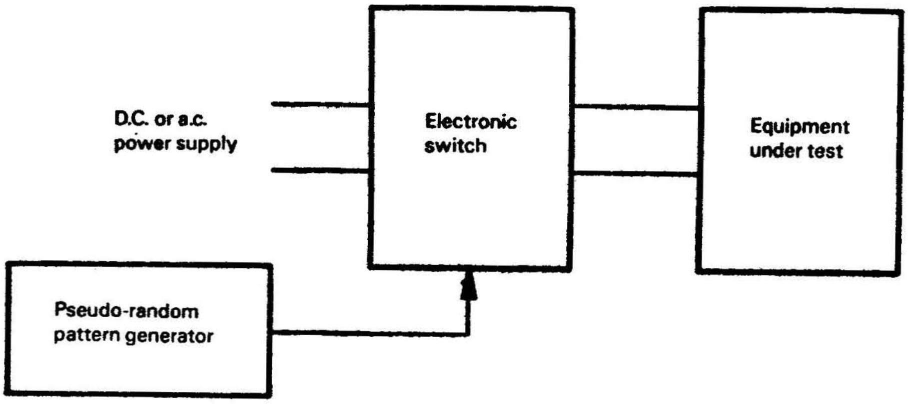


FIG. 6 TEST CIRCUIT FOR TESTING POWER SUPPLY INTERRUPTIONS

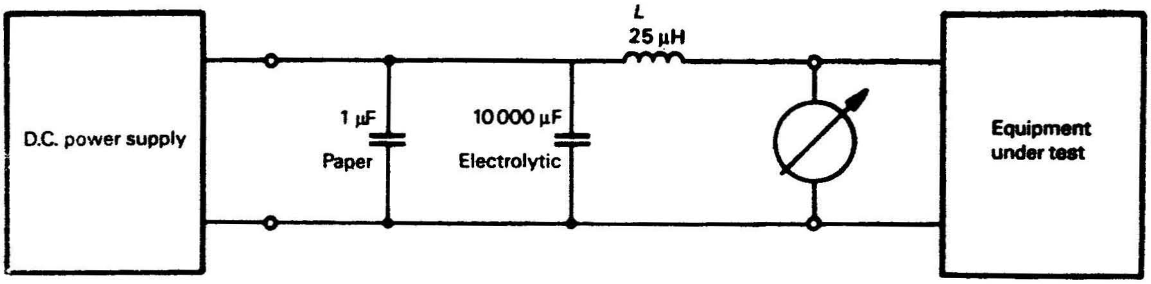


FIG. 7 TEST CIRCUIT FOR MEASURING REFLECTED NOISE

The low pass filter LC decouples the equipment from the power supply source.

3.4 Reverse Polarity

No special arrangement is needed for the reverse polarity test. Before testing, check that the equipment is protected against reverse polarity.

4 TELEPROTECTION SYSTEM PERFORMANCE TEST

A teleprotection channel may be exposed to various kinds of noise depending on the transmission medium used.

Testing the security and to some degree also testing the dependability is a time consuming procedure. It is, therefore, very important to choose a procedure which will give a good measure of the performance of the channel within a reasonable time. The chosen procedure shall also be easy to repeat and the test instruments easy to obtain.

One way to fulfil all the above-mentioned requirements is to adopt a test procedure using white noise. Both the security and the dependability can be tested in relation to the S/N ratio when the noise is white noise. In some special cases, results are not comparable with measurements made with impulse noise.

The noise shall be referred to a fixed bandwidth. Bandwidths smaller than approximately 1 kHz shall not be used since this will result in uncertainty of the measured level, 4 kHz bandwidth is recommended, but other bandwidths may be used when defined. The chosen bandwidth is used irrespectively of the channel tested. All noise measurements shall be unweighted.

Additional tests may be carried out using variable tones.

4.1 Dependability

Noise may disrupt a teleprotection channel by delaying a genuine command signal or by preventing the receiver from delivering a command.

It is, therefore, important to test the receiver for various S/N ratios. Dependability versus S/N ratio shall be measured by comparing the number of commands delivered from the receiver within an acceptable actual transmission time with the number of commands sent from the transmitter. The received commands shall have a specified minimum duration.

If a longer transmission time can be accepted, dependability will increase. Within a given time t a number of commands are sent and received:

N_T = number of commands sent,

N_R = number of commands received.

The dependability is a function of 'the probability of missing command P_{uc}'.

The estimated probability of missing command can be stated as:

$$P_{uc} \approx \frac{N_T - N_R}{N_T} = 1 - \frac{N_R}{N_T}$$

When measuring the dependability versus S/N ratio for various transmission times a family of curves similar to those given in Fig. 8 will be obtained.

Continuous white noise is used and the noise bandwidth shall be indicated.

When measuring dependability a test set-up similar to Fig. 9 is recommended.

To obtain a family of curves as in Fig. 8 it is necessary to send a sufficient number of commands to give a statistically significant measurement. The higher the dependability it is intended to measure, the higher the number of commands it is necessary to send.

Each command shall have a minimum duration consistent with the maximum tolerable transmission time. The interval between successive commands shall be sufficient to allow the receiver to recover. This will normally result in a repetition rate of 1 to 10 commands per second.

For all applications the received command shall be longer than a specified duration:

- for tripping : 10 ms;
- for blocking : 100 ms.

Noise blocking devices in the receiver will influence the dependability for high noise levels. It may be interesting to assess this influence and sometimes it may be of value to measure the dependability at high noise levels both with and without the noise blocking device in action.

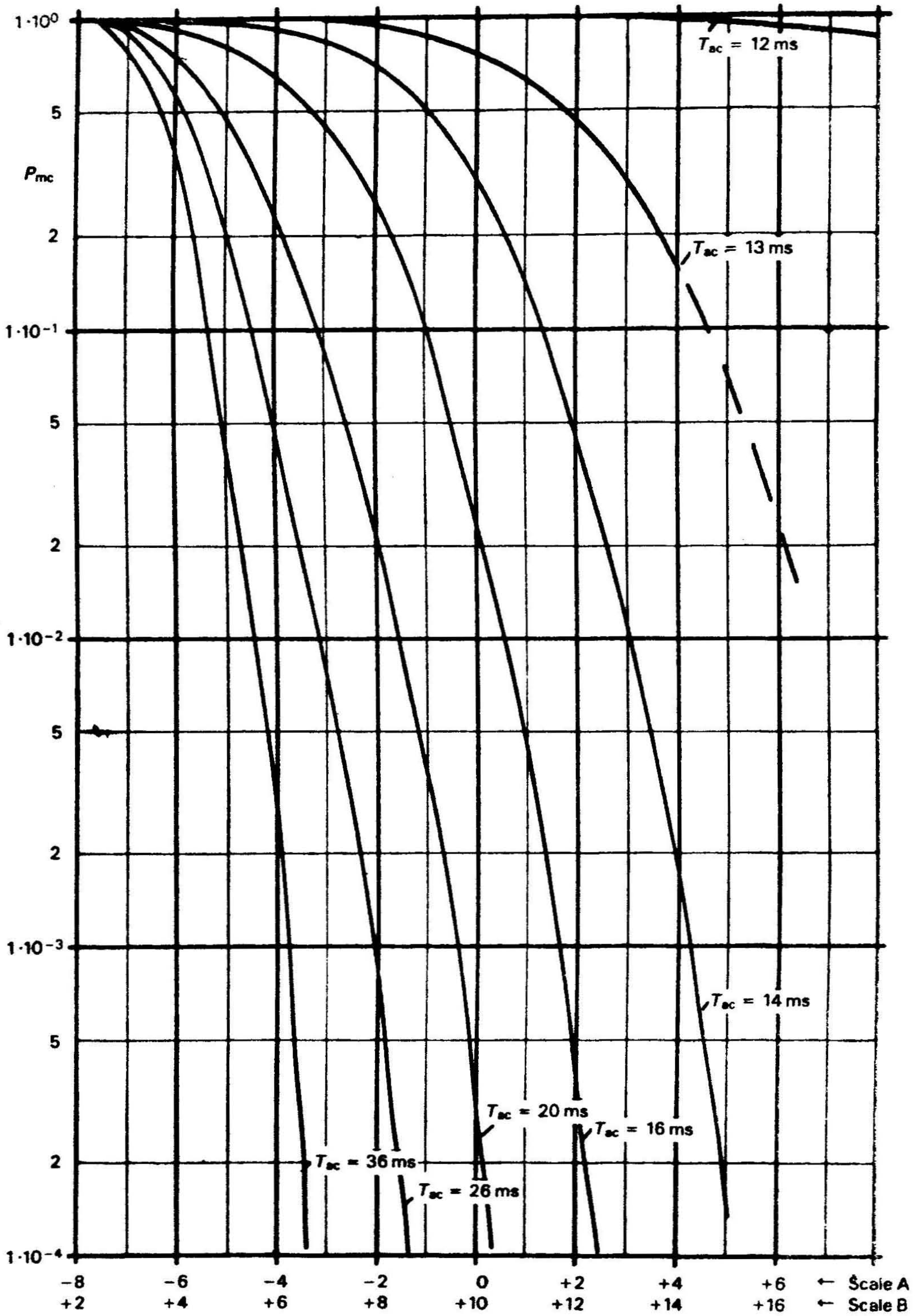
For each setting of the channel, curves showing the dependability versus S/N ratio may be given. It is up to the manufacturer to give these.

The curves shall at least be given in the range T_0 and 3 × T_0.

The dependability can be measured at two different receive levels:

1) with nominal signal level at the receiver input; and
2) with nominal signal level at the receiver input, but with the line attenuation suddenly increased by 10 dB (provided an acceptable S/N ratio is maintained) when a command signal is sent.

This test should be subject to agreement between the user and the manufacturer and may not be required in other applications than PLC.



Scale A = noise bandwidth 4 000 Hz (base band)
Scale B = noise bandwidth 400 Hz (channel band)
Actual transmission time T_{ac} as parameter

FIG. 8 EXAMPLES OF PROBABILITY OF MISSING COMMAND *Versus* S/N FOR A 200-BAUD CHANNEL

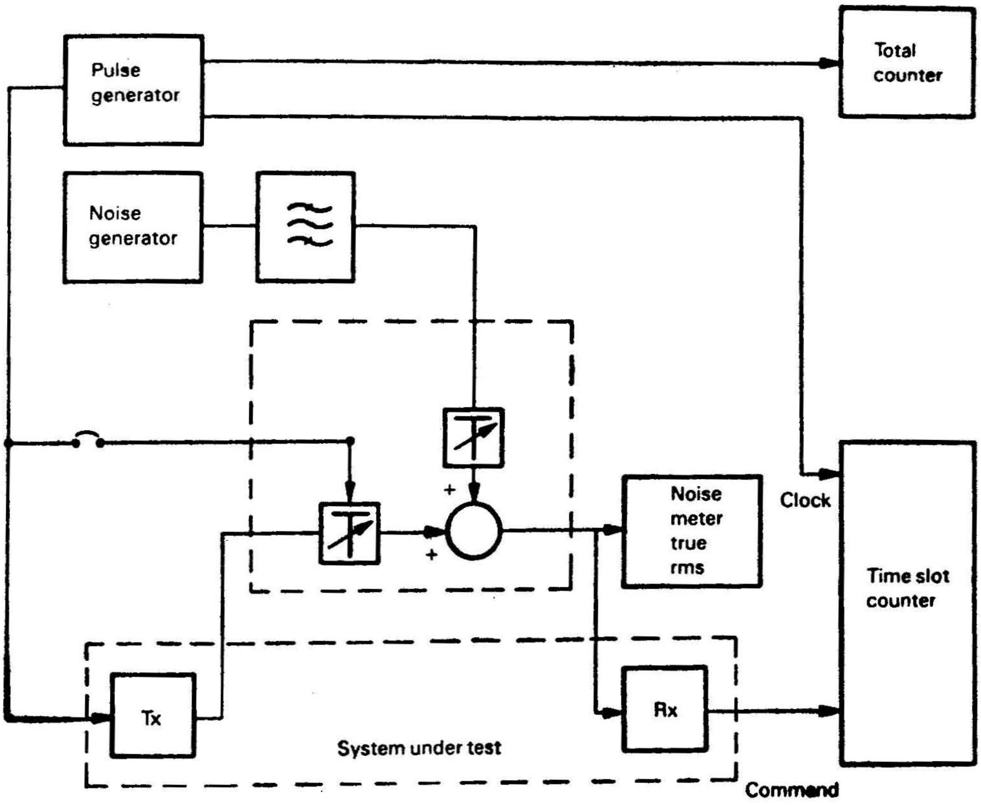


FIG. 9 TEST SET-UP FOR DEPENDABILITY MEASUREMENT

4.2 Security

The most serious noise for a teleprotection channel consists of bursts of impulse noise of high level. Bursts of white noise are used instead for testing the security, the duration of the noise bursts (T_B) being a time reference. A duration of 200 ms and an interval of 200 ms are recommended.

Within a given time, a number of noise bursts are applied and a number of unwanted commands appear at the receiver output.

N_B = number of noise bursts applied;

N_{uc} = number of unwanted commands at the receiver output.

The security is a function of the 'probability of unwanted command P_{uc}'.

The estimate of P_{uc} can be stated as:

$$P_{uc} \approx \frac{N_{uc}}{N_B}$$

For measuring security a test set-up similar to that in Fig. 10 is recommended.

The number of unwanted commands recorded and the total number of noise bursts applied shall be recorded in relation to the S/N ratio. This will result in a characteristic similar to curve *a* in Fig. 11 if no blocking device is included in the receiver.

Only one unwanted command per burst shall be counted and only if its duration is longer than a specified time, for example 5 ms.

When using blocking devices in the receiver a characteristic similar to curve *b* of Fig. 11 may result. Depending on the threshold level of the blocking device it will be time consuming to measure an actual characteristic similar to curve *b*, because the measured P_{uc} will be very low.

Curves for the 'probability of unwanted command P_{uc}' should be measured at nominal receive level.

Curves shall be given for each setting recommended for the channel.

4.3 Transmission Time

A test set-up for measuring transmission time is given in Fig. 12. Recommended measuring

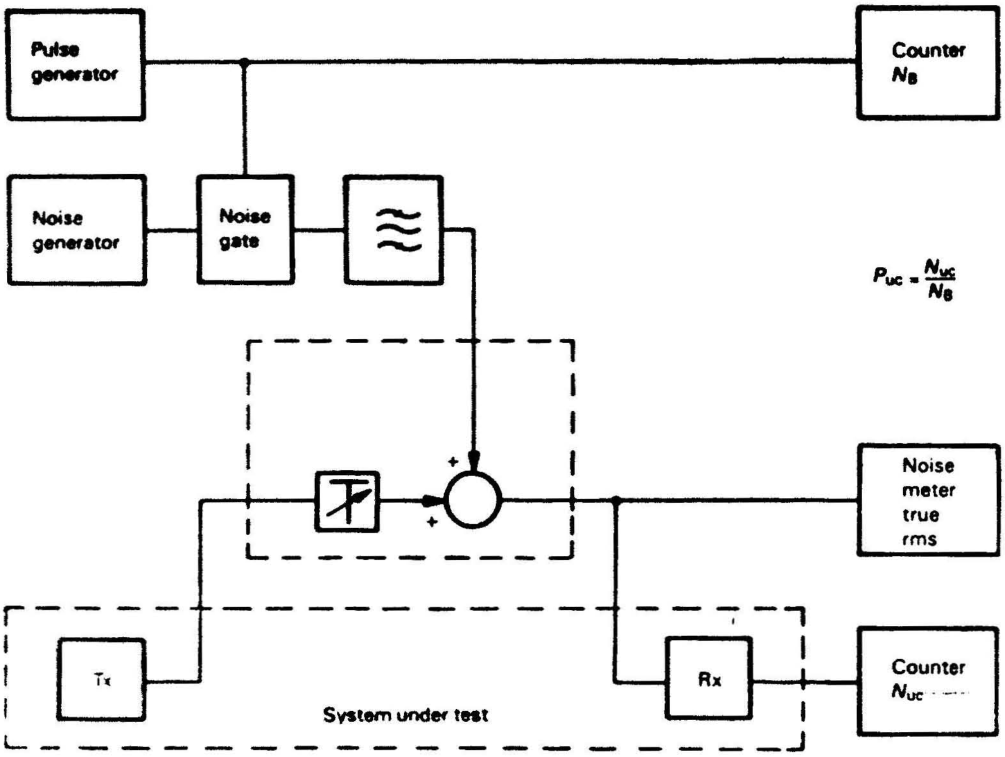


FIG. 10 TEST SET-UP FOR SECURITY MEASUREMENT

equipment consists of a time measuring device and an adjustable and switchable attenuator with the same impedance as for the teleprotection channel.

The transmission time can be measured under the following conditions:

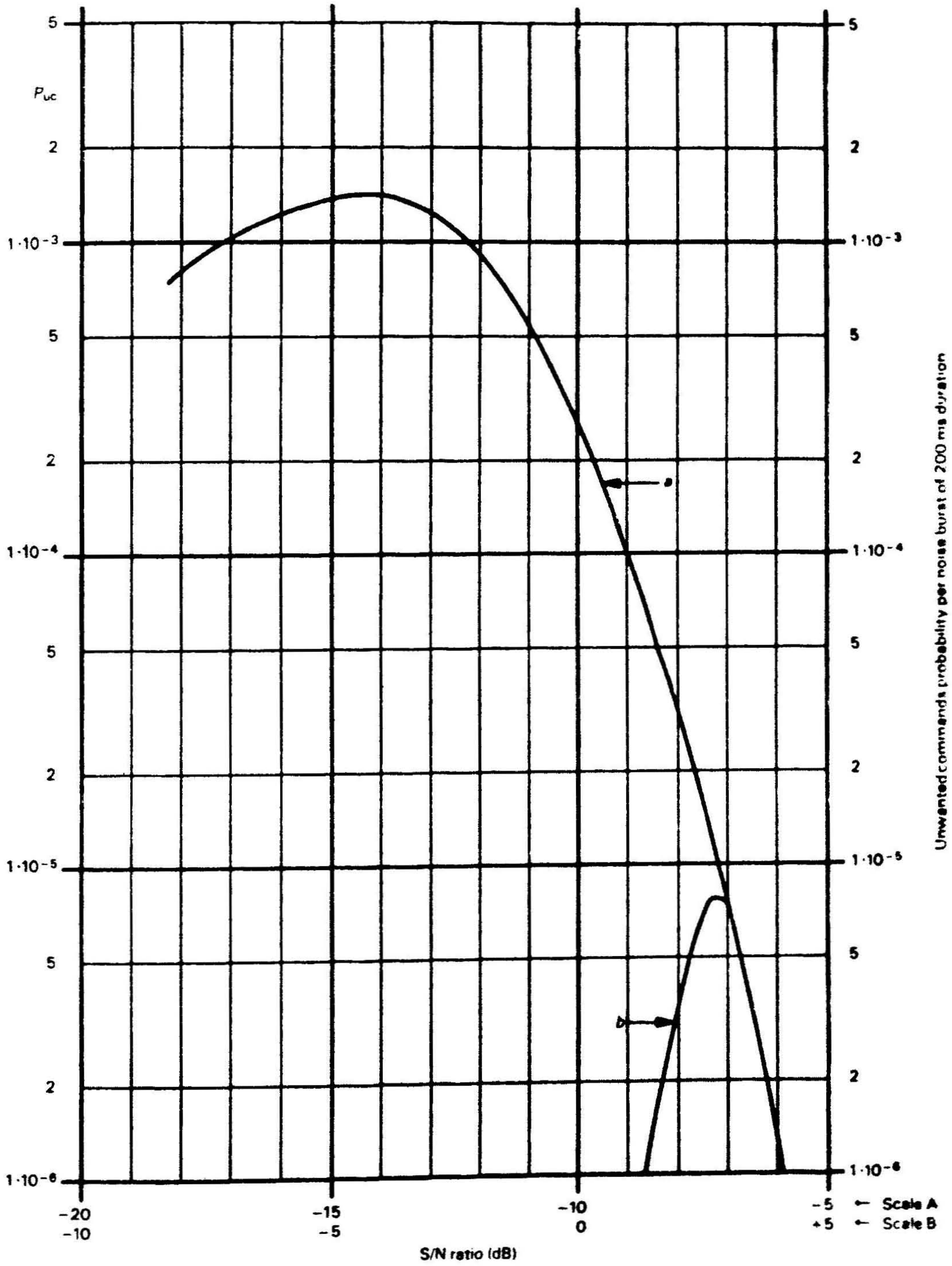
1) with nominal signal levels at the transmitter output and the receiver input. The measured time is T_0;

2) with nominal signal level at the transmitter output and the line attenuation increased by 10 dB (provided an acceptable S/N ratio is maintained) simultaneously with a command being sent.

This test should be subject to agreement between the user and the manufacturer and may not be required in other applications than PLC.

4.4 Interference by Discrete Frequencies

To measure the sensitivity of the teleprotection receiver to interference from discrete frequencies a test set-up similar to that in Fig. 13 is recommended.



Scale A = noise bandwidth 4 000 Hz (base band)
Scale B = noise bandwidth 400 Hz (channel band)
Curve *a* : Without noise blocking device
Curve *b* : With noise blocking device

FIG. 11 EXAMPLES OF PROBABILITY OF UNWANTED COMMANDS *Versus* S/N FOR 200-BAUD CHANNEL

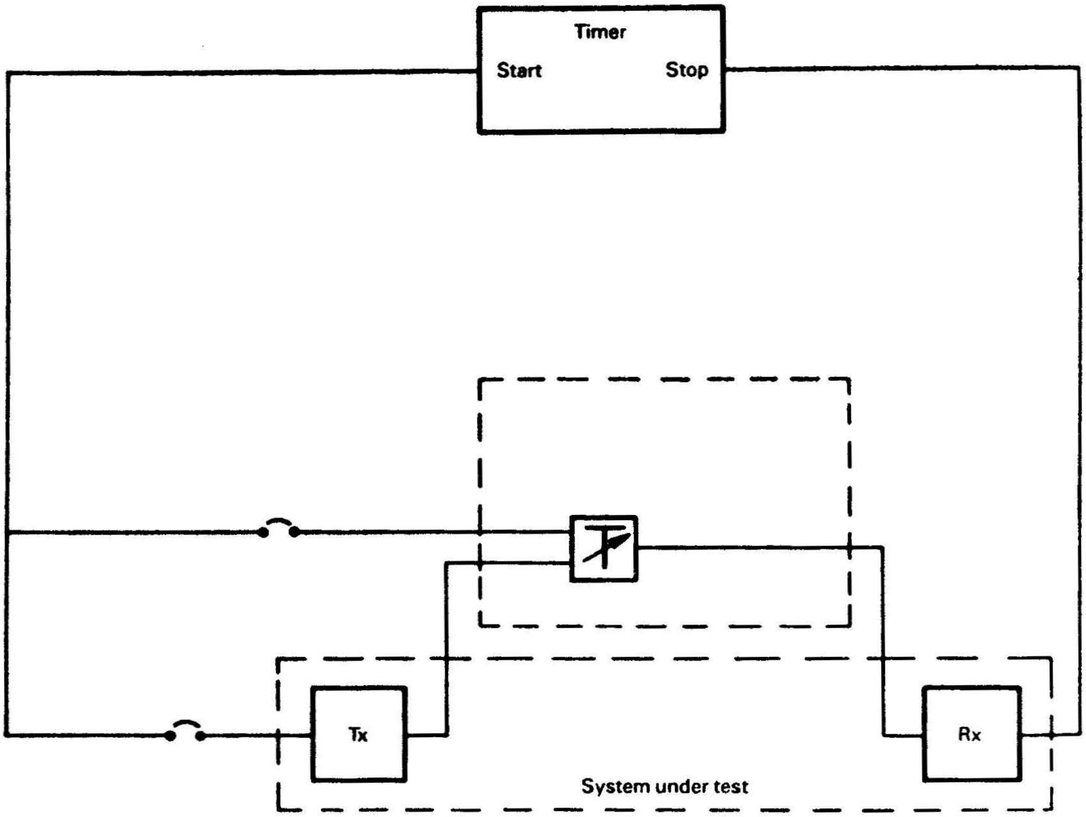


FIG. 12 TEST SET-UP FOR MEASURING TRANSMISSION TIME

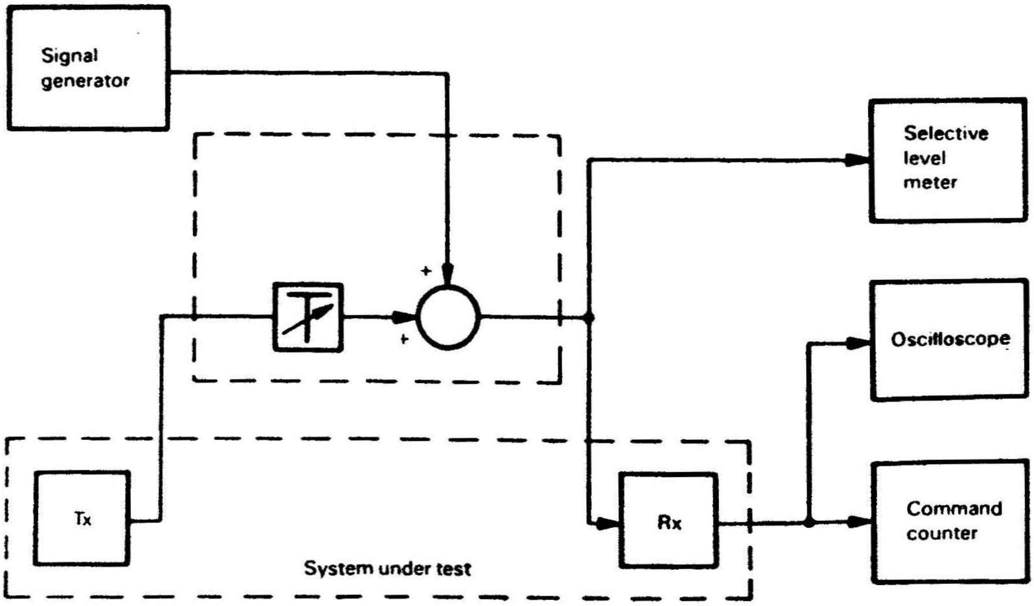


FIG. 13 TEST SET-UP FOR MEASURING INTERFERENCE BY DISCRETE FREQUENCIES

Two series of measurements shall be carried out, the first one when transmitting a guard signal, the second one when transmitting a command signal. In each case an interfering signal, injected at the input of the receiver, shall be swept slowly over the whole frequency band used. Several sweeps with different levels of the interfering signal shall be done when:

1) *the transmitter is sending a guard signal*

   Command output conditions shall be monitored for unwanted commands when the interfering signal is swept over the whole frequency band used. The following levels of the interfering signal shall at least be used : the ratio of the guard signal level to the level of the interfering signal shall be – 6 dB, 0 dB, + 6 dB. Additional sweeps with other interfering signal levels may be made, in order to verify both frequency and level dependence of this interference.

2) *the transmitter is sending a command signal*

   Command output conditions shall be monitored for loss of command when the interfering signal is swept over the whole frequency band. The same levels for the interfering signal (as given under Item 1) shall be used.

4.5 Interference by Frequency Deviation

The teleprotection equipment sometimes used a telecommunication circuit where frequency deviation may occur. A power disturbance or change from primary to secondary route may cause temporary frequency displacement of the standby frequency by a few hertz.

Only when agreed upon between the user and the manufacturer shall a frequency deviation test be carried out.

A low frequency from the teleprotection transmitter is translated to a higher frequency by the frequency f_s. Only one sideband is transmitted through the band pass filter following the modulator. At the receive side, the frequency f_r will demodulate the high frequency back to low frequency in the demodulator. A low pass filter after the demodulator will only allow the low frequencies to arrive at the teleprotection receiver.

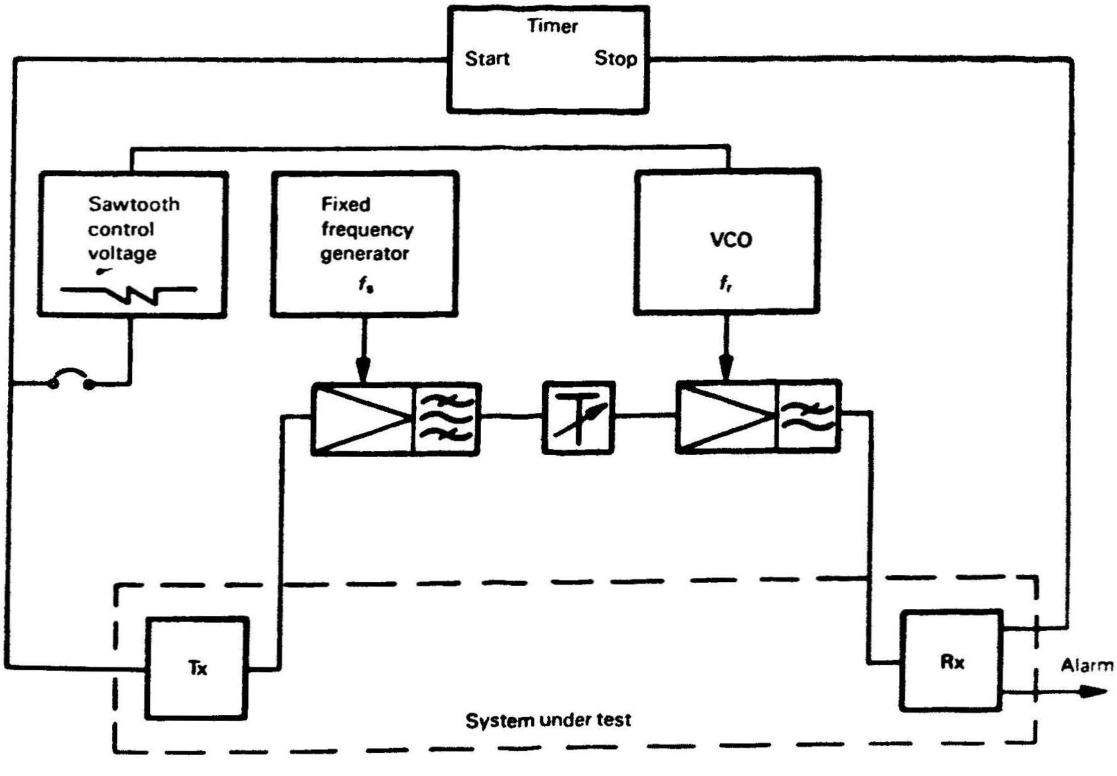


FIG. 14 TEST SET-UP FOR MEASURING INTERFERENCE BY FREQUENCY DEVIATION

Frequency generator f_r shall be designed such that a variable control voltage will cause change in frequency [voltage controlled oscillator (VCO)].

When using the test set-up shown in Fig. 14, the following measurements shall be performed. The frequency f_r shall be changed by the application of a sawtooth control voltage. A sawtooth waveform similar to that in Fig. 15 may be used.

The change in frequency of f_r shall be varied from 0 to $\pm B$ (B being the frequency deviation agreed upon between the user and the manufacturer). The teleprotection receiver shall be monitored for loss of guard, receipt of unwanted commands and alarm performance.

4.6 Checking Alarm Functions

When the teleprotection equipment is unable to operate correctly, an external alarm shall be given.

The equipment shall be checked to see if the alarm is operating correctly. An alarm shall be given when:

a) the guard signal is cut off from the receiver and no command signal appears at the receiver within a specified time given by the manufacturer (some seconds);

b) heavy noise blocks receiver for a time longer than a specified time given by the manufacturer (some seconds), and

c) the manufacturer may specify other situations (e.g. transmitter failure) where an alarm shall be given. For these situations the function of the alarm shall also be tested.

4.7 Multicommand Equipment

A multicommand teleprotection equipment has normally a common guard signal and two or more command signals.

Testing of the security of the command signals shall be done in the same way as described in **4.2**. Each command signal shall be tested.

Testing of the dependability shall be done as described in **4.1** for each of the command signals.

When testing the dependability of one command signal, the security of unwanted commands at each of the other command signals shall be tested at the same time.

4.8 Additional Tests

Additional measurements may be agreed upon between the user and the manufacturer.

4.9 Supplimentary Information

Additional information is given in Annex A.

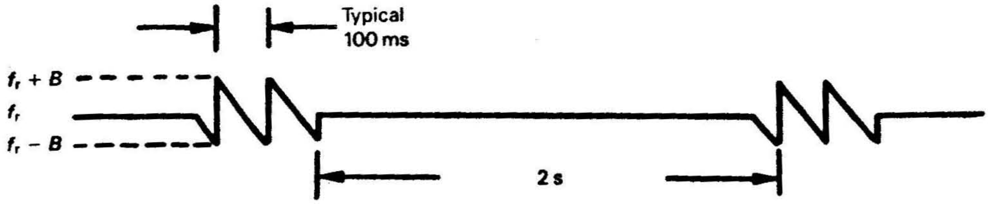


FIG. 15 FREQUENCY DEVIATION *Versus* TIME FOR TEST SET-UP IN FIG. 14

ANNEX A

(*Clause* 4.9)

ADDITIONAL DATA FOR TELEPROTECTION SYSTEM PERFORMANCE TESTS

A-1 COMPARISON OF NOISE LEVELS

White noise levels measured at different bandwidths can be compared by using the following formula:

$$P_N\ (\ x\mathrm{kHz}\ )\ \mathrm{dB} = P_N\ (\ 4\ \mathrm{kHz}\ )\ \mathrm{dB} - 10\ \lg \frac{4\ (\ \mathrm{kHz}\ )}{x\ (\ \mathrm{kHz}\ )}$$

A-2 SECURITY AND DEPENDABILITY MEASUREMENTS

For the measurements of security and dependability a reasonable certainty is asked for. The certainty depends on the number of events observed.

If N = total number of attempts made, and

E = number of events observed

then the probability of getting the events observed with a confidence level of 95% given by the following approximation:

$$P = \frac{E}{N} \left(1 \pm \frac{2}{\sqrt{E}} \right)$$

Increasing the number of E will result in a smaller range of uncertainty.

An illustration of how this method will work is given in Fig. 16. The probability P is given in logarithmic scale on the Y axis. Spread over the graph we have five measurements made with N = 250, 1 000, 4 000, 16 000 and 64 000. For each value of N various values of E have been chosen. For each value of N the necessary time to measure the whole series is given. In this case, the measurement have been done with eight samples per second.

Figure 17 shows the uncertainty resulting from the number of unwanted command received.

For curve *a*, the dashed lines indicate the uncertainty for a confidence level of 95% when the given unwanted commands are measured. If the number of unwanted commands is reduced by x the uncertainty will increase by $\sqrt{x}$.

For the number of unwanted commands given in Fig. 17, the following hours for each measurement will be needed:

for $P_{uc} = 10^{-3}$, $N = 10^5$, 11.1 h are needed;

$P_{uc} = 10^{-4}$, $N = 5 \cdot 10^5$, 55.5 h (2·25 days) are needed;

$P_{uc} = 10^{-5}$, $N = 3 \cdot 10^6$, 333·3 h (14 days) are needed.

This means that it is not practical to make measurements for $P_{uc} < 10^{-5}$.

A-3 IN-SERVICE TESTING

In principle, a protection signalling equipment should raise an alarm if it is unable to operate correctly. Similarly, if the equipment does not raise an alarm, it should basically be able to operate correctly. Further, the equipment design should be such that a single component failure cannot cause maloperations.

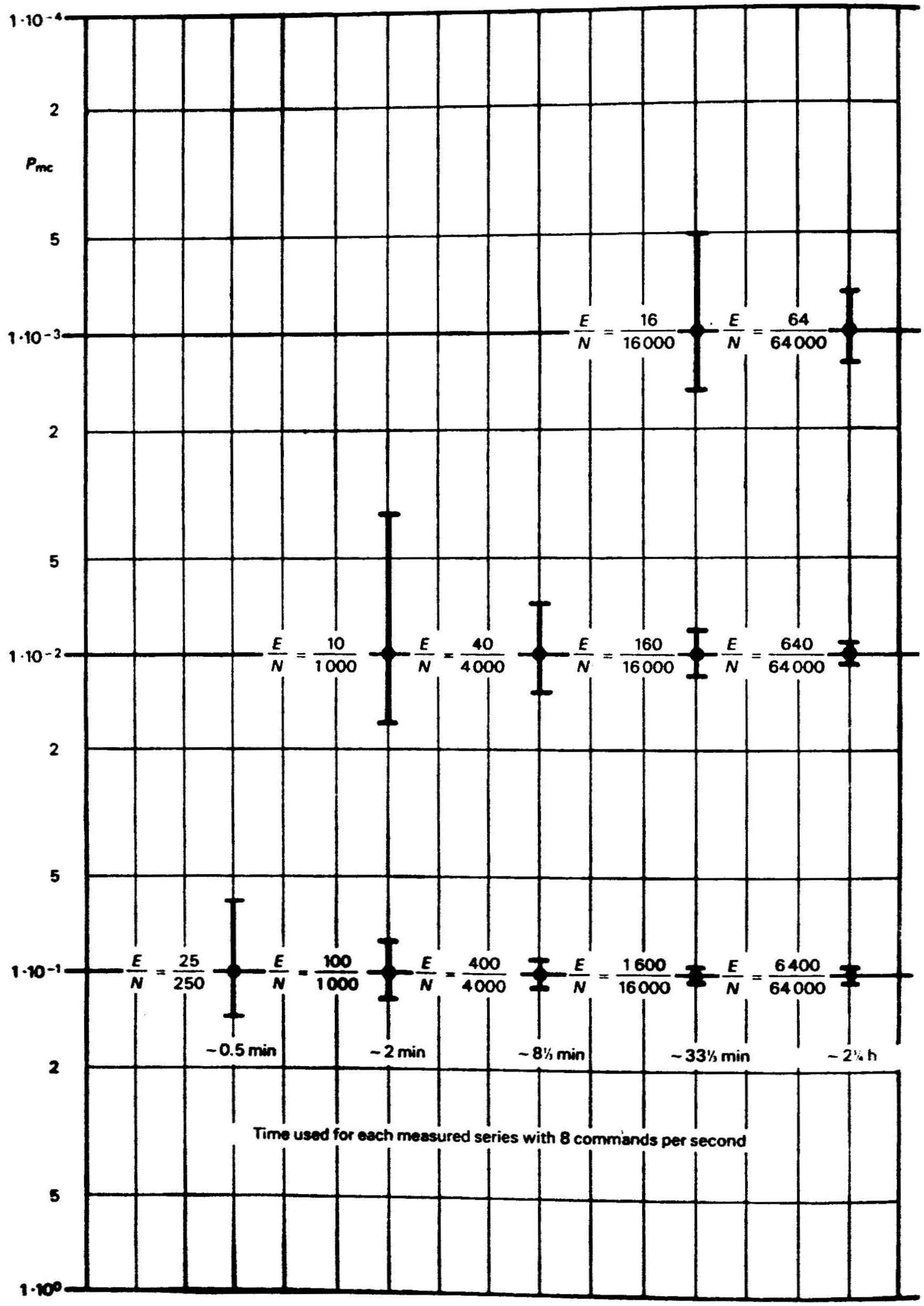
The fact that it is difficult or even impossible to fulfil the above requirements completely has led to the practice of checking all equipment functions by regular in-service tests.

Protection singalling equipment is normally in the 'command off' state, thus the ability to withstand unwanted commands is automatically evaluated during its lifetime.

Since genuine commands are infrequent and rare, the ability to transmit commands correctly should preferably be verified regularly by manual or clock tests.

In any case, test signals should be immediately overridden by genuine command signals.

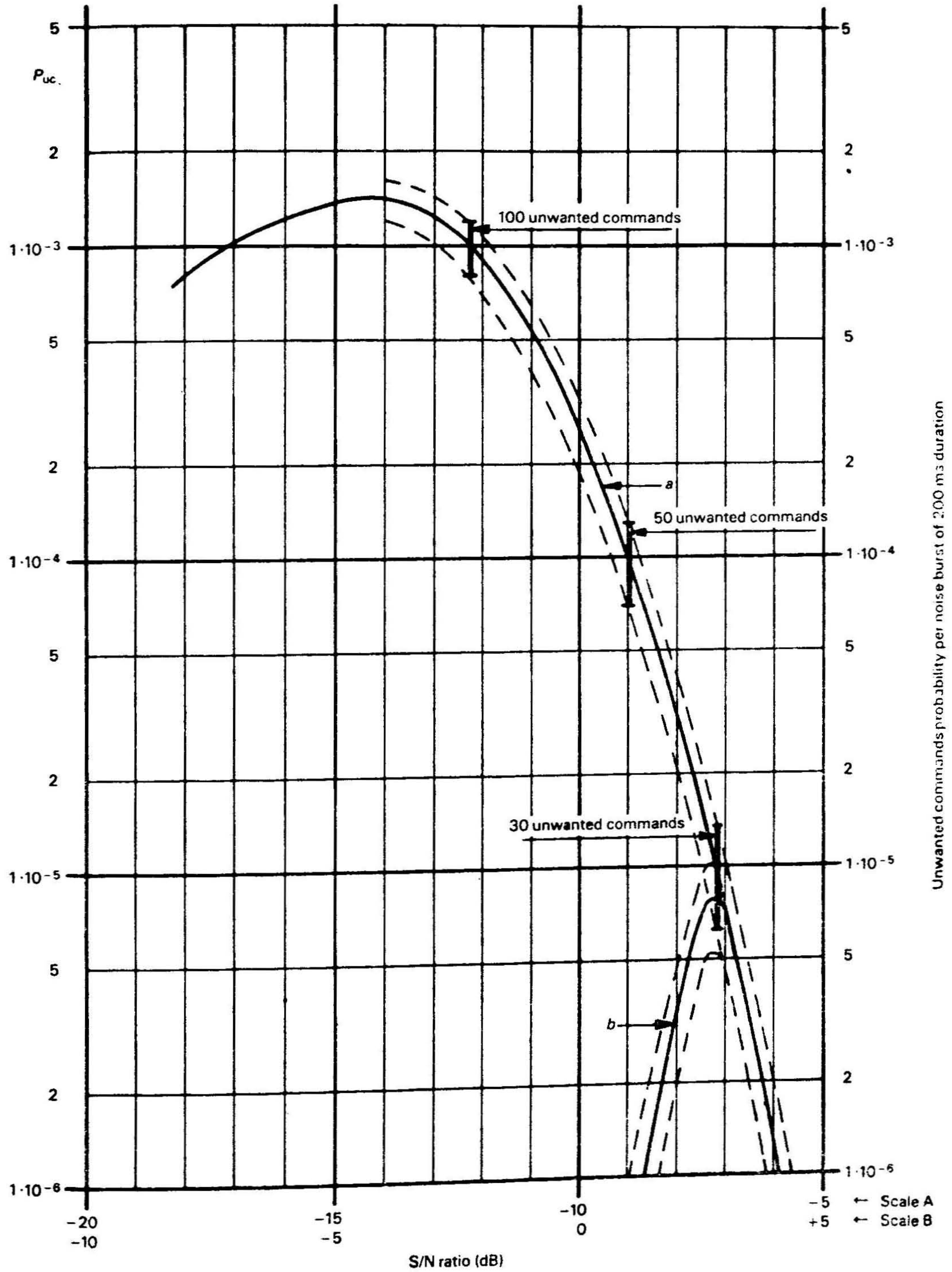
In-service testing by transmission of real commands is possible in blocking and permissive tripping applications, in the latter case with a small risk of unwanted tripping. In intertripping applications, in-service testing of different equipment functions can only be performed if precautions are taken to avoid any unwanted tripping.



E = number of events observed

N = total number of attempts made

FIG. 16 GRAPH SHOWING THE UNCERTAINTY OF THE PROBABILITY FOR A CONFIDENCE LEVEL OF 95% FOR VARIOUS E AND N



Scale A = noise bandwidth 4 000 Hz (base band)

Scale B = noise bandwidth 400 Hz (channel band)

FIG. 17 EXAMPLES OF PROBABILITY OF UNWANTED COMMANDS *Versus* S/N 200-BAND CHANNEL

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act, 1986* to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reproduced in any form without the prior permission in writing of BIS. This does not preclude the free use, in the course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright be addressed to the Director (Publications), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition.

This Indian Standard has been developed from Doc : No. LTD 25 (1437 to 1441).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones : 331 01 31, 331 13 75

Telegrams : Manaksanstha
(Common to all offices)

Regional Offices :

		Telephone
Central :	Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110002	331 01 31 331 13 75
Eastern :	1/14 C. I. T. Scheme VII M, V. I. P. Road, Maniktola CALCUTTA 700054	37 84 99, 37 85 61 37 86 26, 37 86 62
Northern :	SCO 445-446, Sector 35-C, CHANDIGARH 160036	53 38 43, 53 16 40 53 23 84
Southern :	C. I. T. Campus, IV Cross Road, MADRAS 600113	235 02 16, 235 04 42 235 15 19, 235 23 15
Western :	Manakalaya, E9 MIDC, Marol, Andheri (East) BOMBAY 400093	632 92 95, 632 78 58 632 78 91, 632 78 92

Branches : AHMADABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. PATNA. THIRUVANANTHAPURAM.

Printed at New India Printing Press, Khurja, India